Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended) A network access device comprising:

a plurality of input ports;

a memory for storing data packets received on the plurality of input ports;

a switching fabric configured for packet switching of the data packets to at least one output port; and

control logic adapted to:

examine a first data packet comprising a physical address of a user device coupled to one of the plurality of input ports;

authenticate the physical address;

if the authentication of the physical address indicates the physical address is valid, authenticate one or more user credentials ~~user information~~ provided in a second data packet by a user of the user device after the physical address is authenticated; ~~and~~

if the authentication of the one or more user credentials ~~user information~~ indicates the one or more user credentials ~~user information is~~ are valid, determine ~~and~~ if the network access device has sufficient ~~enough~~ system resources to dynamically configure a user policy;

if the determination indicates the network access device has sufficient system resources, dynamically assign the user policy to the one of the plurality of input ports; and

restrict further traffic on the one of the plurality of input ports in accordance with the user policy; and

if the authentication of the physical address indicates the physical address is invalid, or if the determination indicates insufficient system resources, block traffic on the one of the plurality of ports except for packets related to a user authentication protocol.

2. (Previously Presented) The network access device of claim 1, wherein the physical address comprises a Media Access Control (MAC) address.

3. (Previously Presented) The network access device of claim 1, wherein the control logic is adapted to authenticate the user information in accordance with an IEEE 802.1x protocol.

4. (Previously Presented) The network access device of claim 1, wherein the user policy identifies an access control list.

5. (Previously Presented) The network access device of claim 1, wherein the user policy includes an access control list.

6. (Previously Presented) The network access device of claim 1, wherein the user policy identifies a Media Access Control (MAC) address filter.

7. (Previously Presented) The network access device of claim 1, wherein the user policy includes a Media Access Control (MAC) address filter.

8. (Currently Amended) The network access device of claim 1, wherein the control logic is adapted to send the one or more user credentials ~~information~~ to an authentication server and to receive an accept message from the authentication server if the user information is valid.

9. (Previously Presented) The network access device of claim 8, wherein the authentication server comprises a Remote Authentication Dial-In User Service (RADIUS) server.

10. (Previously Presented) The network access device of claim 8, wherein the accept message includes the user policy.

11. (Currently Amended) The network access device of claim 1, wherein the control logic is further adapted to assign the one of the plurality of input ports to a virtual local area network (VLAN) associated with the one or more user credentials ~~information~~ if the one or more user credentials ~~information is~~ are valid.

12. (Currently Amended) The network access device of claim 11, wherein the control logic is adapted to receive a message from an authentication server, wherein the message comprises a VLAN identifier (ID) associated with the one or more user credentials ~~information~~, and to assign the one of the plurality of input ports to a VLAN associated with the VLAN ID.

13. (Currently Amended) A computer implemented method for providing network security, the method comprising:

at a network access device comprising a plurality of input ports and configured for packet switching of data packets, examining a first data packet comprising a physical address of a user device coupled to one of the plurality of input ports;

authenticating the physical address;

if the authentication of the physical address indicates the physical address is valid, authenticating one or more user credentials ~~user information~~ provided in a second data packet by a user of the user device after the physical address is authenticated; ~~and~~

if the authentication of the one or more user credentials ~~user information~~ indicates the one or more user credentials ~~user information is~~ are valid, determining ~~and~~ if the network access device has sufficient ~~enough~~ system resources to dynamically configure a user policy;

if the determining indicates sufficient system resources, dynamically assigning the user policy to the one of the plurality of input ports and restricting further traffic on the port in accordance with the user policy; and

if the authentication of the physical address indicates the physical address is invalid, or if the determining indicates insufficient system resources, blocking traffic on the one of the plurality of ports except for packets related to a user authentication protocol.

14. (Previously Presented) The method of claim 13, wherein the authenticating a physical address comprises authenticating a Media Access Control (MAC) address.

15. (Previously Presented) The method of claim 13, wherein the authenticating the user information comprises authenticating the user information in accordance with an IEEE 802.1x protocol.

16. (Previously Presented) The method of claim 13, wherein the restricting access comprises restricting access to the one of the plurality of input ports in accordance with an access control list.

17. (Previously Presented) The method of claim 13, wherein the restricting access comprises restricting access to the one of the plurality of input ports in accordance with a Media Access Control (MAC) address filter.

18. (Currently Amended) The method of claim 13, wherein the authenticating the user information comprises:

sending the one or more user credentials ~~information~~ to an authentication server; and

receiving an accept message from the authentication server if the one or more user credentials ~~information is~~ are valid.

19. (Previously Presented) The method of claim 18, wherein the authentication server comprises a Remote Authentication Dial-In User Service (RADIUS) server.

20. (Previously Presented) The method of claim 18, wherein the receiving an accept message comprises receiving an accept message that includes the user policy.

21. (Currently Amended) The method of claim 13, further comprising:

assigning the port to a virtual local area network (VLAN) associated with the one or more user credentials ~~information~~ only if the one or more user credentials ~~information is~~ are valid.

22. (Previously Presented) The method of claim 21, wherein the assigning the port to a VLAN comprises:

receiving a message from an authentication server, wherein the message comprises a VLAN identifier (ID) associated with the user information; and

assigning the port to a VLAN associated with the VLAN ID.

23. (Currently Amended) A network system, comprising:

a network access device comprising a plurality of input ports and configured for packet switching of data packets in a data communications network; and

a user device coupled to a port of the network access device;

wherein the network access device is adapted to:

examine a first data packet comprising a physical address of a user device coupled to one of the plurality of input ports;

authenticate the physical address;

if the authentication of the physical address indicates the physical address is valid, authenticate one or more user credentials ~~user information~~ provided in a second

data packet by a user of the user device after the physical address is authenticated; ~~and~~

if the authentication of the one or more user credentials ~~user information~~ indicates the one or more user credentials ~~user information is~~ are valid, determine ~~and~~ if the network access device has sufficient ~~enough~~ system resources to dynamically configure a user policy;

if the determination indicates the network access device has sufficient system resources, dynamically assign the user policy to the one of the plurality of input ports; and restrict further traffic on the one of the plurality of input ports in accordance with the user policy; and

if the authentication of the physical address indicates the physical address is invalid, or if the determination indicates insufficient system resources, block traffic on the one of the plurality of ports except for packets related to a user authentication protocol.

24. (Previously Presented) The system of claim 23, wherein the physical address comprises a Media Access Control (MAC) address.

25. (Previously Presented) The system of claim 23, wherein the network access device is adapted to authenticate the user information in accordance with an IEEE 802. lx protocol.

26. (Previously Presented) The system of claim 23, wherein the user policy identifies an access control list.

27. (Previously Presented) The system of claim 23, wherein the user policy includes an access control list.

28. (Previously Presented) The system of claim 23, wherein the user policy identifies a Media Access Control (MAC) address filter.

29. (Previously Presented) The system of claim 23, wherein the user policy includes a Media Access Control (MAC) address filter.

30. (Currently Amended) The system of claim 23, further comprising:
an authentication server coupled to the data communications network;
wherein the network access device is adapted to send the one or more user credentials ~~information~~ to an authentication server and to receive an accept message from the authentication server if the user information is valid.

31. (Previously Presented) The system of claim 30, wherein the authentication server comprises a Remote Authentication Dial-In User Service (RADIUS) server.

32. (Previously Presented) The system of claim 30, wherein the accept message includes the user policy.

33. (Currently Amended) The system of claim 23, wherein the network access device is further adapted to assign the one of the plurality of input ports to a virtual local area network

(VLAN) associated with the one or more user credentials ~~information~~ if the one or more user credentials ~~information is~~ are valid.

34. (Previously Presented) The system of claim 33, further comprising:

an authentication server coupled to the data communications network;

wherein the network access device is adapted to receive a message from the authentication server, wherein the message comprises a VLAN identifier (ID) associated with the user information, and to assign the port to a VLAN associated with the VLAN ID if the user information is valid.

35. (Currently Amended) The network access device of claim 2 wherein the control logic is further configured to:

if authentication of the MAC address indicates the MAC address is invalid,

drop packets from the user device; or

disable the port;

~~if authentication of the user information indicates the user information is invalid, block all traffic on the port except for packets related to a user authentication protocol;~~

if authentication of user information indicates the user information is valid, determine whether the user is associated with a VLAN supported by the network access device;

if the user is not associated with the VLAN,

assign the port to a port default VLAN; and

block all traffic on the port except for packets related to the user authentication protocol; and

if the user is associated with the VLAN,

assign the port to the VLAN associated with the user; and

forward packets from the user device.

36. (Currently Amended) The method of claim 14, further comprising:

if the authenticating of the MAC address indicates the MAC address is invalid,

dropping packets from the user device; or

disabling the port;

~~if the authenticating user information indicates the user information is invalid, blocking all traffic on the port except for packets related to a user authentication protocol;~~

if the authenticating user information indicates the user information is valid, determining whether the user is associated with a VLAN supported by the network access device;

if the determining indicates the user is not associated with the VLAN,

assigning the port to a port default VLAN; and

blocking all traffic on the port except for packets related to the user authentication protocol; and

if the determining indicates the user is associated with the VLAN,

assigning the port to the VLAN associated with the user; and

forwarding packets from the user device.

37. (Currently Amended) The network system of claim 24 wherein the network access device is further adapted to:

if authentication of the MAC address indicates the MAC address is invalid,

dropping packets from the user device; or

disabling the port;

~~if authentication of the user information indicates the user information is invalid, block all traffic on the port except for packets related to a user authentication protocol;~~

if authentication of user information indicates the user information is valid, determine whether the user is associated with a VLAN supported by the network access device;

if the user is not associated with the VLAN,

assign the port to a port default VLAN; and

block all traffic on the port except for packets related to the user authentication protocol; and

if the user is associated with the VLAN,

assign the port to the VLAN associated with the user; and

forward packets from the user device.

38. (Previously Presented) An apparatus comprising:

a plurality of input ports;

a memory for storing data packets received on the plurality of input ports;

a switching fabric configured for packet switching of the data packets to at least one output port; and

control logic adapted to:

examine a first data packet comprising a physical address of a user device coupled to one of the plurality of input ports;

authenticate the ~~a~~ physical address;

drop packets from the user device if the physical address is invalid;

authenticate user information provided in a second data packet by a user of the user device after the physical address is authenticated;

if the authentication of the user information indicates the user information is invalid, block all traffic on the one of the plurality of input ports except for packets related to a user authentication protocol;

if the authentication of the user information indicates the user information is valid, determine whether the user is associated with a VLAN supported by the apparatus by receiving a message from an authentication server, wherein the message comprises a VLAN identifier (ID) associated with the user information;

if the user is not associated with the VLAN,

assign the one of the plurality of input ports to a port default VLAN; and

block all traffic on the one of the plurality of input ports except for packets related to the user authentication protocol; and

if the user is associated with the VLAN and if the apparatus has enough system resources to dynamically configure a user policy associated with the user information,

assign the one of the plurality of ports to the VLAN associated with the user; and

restrict access to the one of the plurality of input ports in accordance with the user policy.

39. (Previously Presented) The apparatus of claim 38, wherein the apparatus comprises a switch.

40. (Previously Presented) A computer implemented method for providing network security, the method comprising:

at a network access device comprising a plurality of input ports and configured for packet switching of data packets, examining a first data packet comprising a physical address of a user device coupled to one of the plurality of input ports;

authenticating the ~~a~~ physical address;

dropping packets from the user device if the physical address is invalid;

authenticating user information provided in a second data packet by a user of the user device after the physical address is authenticated;

if the authenticating of the user information indicates the user information is invalid, blocking all traffic on the port except for packets related to a user authentication protocol;

if the authenticating of the user information indicates the user information is valid, determining whether the user is associated with a VLAN supported by the network access device by receiving a message from an authentication server, wherein the message comprises a VLAN identifier (ID) associated with the user information;

if the user is not associated with the VLAN,

assigning the one of the plurality of input ports to a port default VLAN; and

blocking all traffic on the one of the plurality of input ports except for packets related to the user authentication protocol; and

if the user is associated with the VLAN and if the network access device has enough system resources to dynamically configure a user policy associated with the user information, assigning the one of the plurality of ports to the VLAN associated with the user; and

restricting access to the one of the plurality of input ports in accordance with the a user policy.

41. (Previously Presented) The method of claim 40, wherein the network access device comprises a switch.

42. (Previously Presented) A network system, comprising:

a network access device comprising a plurality of input ports and configured for packet switching of data packets in a data communications network; and

a user device coupled to a port of the network access device, wherein the network access device is adapted to:

examine a first data packet comprising a physical address of a user device coupled to one of the plurality of input ports;

authenticate the physical address;

drop packets from the user device if the physical address is invalid;

authenticate user information provided in a second data packet by a user of the user device after the physical address is authenticated;

if the authentication of the user information indicates the user information is invalid, block all traffic on the port except for packets related to a user authentication protocol;

if the authentication of the user information indicates the user information is valid, determine whether the user is associated with a VLAN supported by the network access device by receiving a message from an authentication server, wherein the message comprises a VLAN identifier (ID) associated with the user information;

if the user is not associated with the VLAN,

assign the one of the plurality of input ports to a port default VLAN; and

block all traffic on the one of the plurality of input ports except for packets related to the user authentication protocol; and

if the user is associated with the VLAN and if the network access device has enough system resources to dynamically configure a user policy associated with the user information,

assign the one of the plurality of ports to the VLAN associated with the user; and

restrict access to the one of the plurality of input ports in accordance with the a user policy.

43. (Previously Presented) The network system of claim 42, wherein the network access device comprises a switch.

44. (Previously Presented) The device of Claim 1 wherein the user information comprises a user name and a password.

45. (Previously Presented) The method of Claim 13 wherein the user information comprises a user name and a password.

46. (Previously Presented) The system of Claim 23 wherein the user information comprises a user name and a password.

47. (Previously Presented) The network access device of Claim 1 wherein the control logic is further adapted to:

if the authentication of the user information indicates the user information is invalid, block all traffic on the one of the plurality of input ports except for packets related to a user authentication protocol.

48. (Previously Presented) The method of Claim 13, further comprising:

if the authentication of the user information indicates the user information is invalid, blocking all traffic on the one of the plurality of input ports except for packets related to a user authentication protocol.

49. (Previously Presented) The system of Claim 23 wherein the network access device is further adapted to:

if the authentication of the user information indicates the user information is invalid, block all traffic on the one of the plurality of input ports except for packets related to a user authentication protocol.